UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

LINDABETH RIVERA and JOSEPH WEISS, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	No. 16 C 02714
v.	)	
GOOGLE INC.,	)	Judge Edmond E. Chang
Defendant.	)	

MEMORANDUM OPINION AND ORDER

The Illinois Biometric Information Privacy Act forbids the unauthorized collection and storing of some types of biometric data. 740 ILCS 14/1 *et seq*. A private entity cannot gather and use someone's "biometric identifier"—defined as retinal or iris scans, fingerprints, voiceprints, or hand or face geometry scans—unless that person has consented. *Id.* § 14/10. The Act also bans the non-consensual collection and storage of information (the Act labels it "biometric information") that is "based on" those biometric identifiers. *Id.*

In the months leading up to March 2016, photographs of Lindabeth Rivera were allegedly taken by a "Google Droid device"[1] in Illinois and automatically uploaded to Google Photos, a cloud-based service. R. 40, Rivera First Am. Compl. ¶

[1]Plaintiffs do not ever come right out and say that a "Google Droid device" is a Google smartphone running on Android, but that is what other references in the briefs suggest it is.

27.[2] From there, Rivera claims, Google immediately scanned her facial features to create a unique face "template." *Id.* ¶ 28. Rivera brings suit against Google for a violation of the Biometric Information Privacy Act, arguing that the company took a scan of her facial geometry without her consent. *Id.* ¶¶ 45. Joseph Weiss alleges a violation of the same Act on the same grounds. [3] *See* R. 41, Weiss First Am. Compl. He claims that Google used photographs of him, taken from a Google Droid device in Illinois (in this case his own), to unlawfully create a face scan. *Id.* ¶¶ 27-29. Google now moves to dismiss Rivera's and Weiss's claims under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim.[4] *See* R. 48, Def.'s Mot. to Dismiss. For the reasons discussed below, Google's motion to dismiss is denied.

I. Background

For purposes of evaluating the dismissal motion, the Court must accept as true the allegations in the First Amended Complaints. *Erickson v. Pardus*, 551 U.S. 89, 94 (2007). Between around March 2015 and March 2016, "approximately eleven" photographs of Lindabeth Rivera were taken in Illinois by a Google Photos user on a

[2]Citations to the record are noted as "R." followed by the docket number and the page or paragraph number.

[3]The Court has diversity jurisdiction over Rivera's and Weiss's state-law claims under 28 U.S.C. § 1332. Rivera and Weiss are citizens of Illinois. Rivera First Am. Compl. ¶ 7; R. 41, Weiss First Am. Compl. ¶ 7. Google is a citizen of Delaware (its place of incorporation) and California (its principal place of business). Weiss First Am. Compl. ¶ 8. The amount in controversy requirement is satisfied. If the plaintiffs are contemplated as a potential class, the aggregate claims of thousands of class members could possibly equal or exceed $5,000,000, exclusive of interest and costs. 28 U.S.C. § 1332(d)(6). Even setting aside the class allegation, it is not "legally impossible" for either Weiss or Rivera alone to recover more than $75,000 in this action. *Back Doctors Ltd v. Metro. Prop. & Cas. Ins. Co.*, 637 F.3d 827, 830 (7th Cir. 2011) (amount-in-controversy requirement satisfied unless it is "legally impossible" for a plaintiff to recover that amount).

[4]Rivera's and Weiss's claims were consolidated for the purposes of Google's response. *See* R. 44, Stipulation re Mots. to Dismiss.

Google Droid device. Rivera First Am. Compl. ¶ 27. The person who took the picture was an Illinois resident who had purchased the Droid device in Illinois. *Id.* As soon as the photographs of Rivera were taken, the Droid automatically uploaded them to the cloud-based Google Photos service. *Id.* According to the Complaint, Google immediately scanned each uploaded photograph of Rivera. *Id.* ¶ 28. The scans located her face and zeroed in on its unique contours to create a "template" that maps and records her distinct facial measurements. *Id.* At the time of the automatic upload and face-scan, the photographer's Droid device was still in Illinois and would have had an Illinois-based Internet Protocol (IP) address. *Id.* ¶ 27.

Weiss's experience was similar, except that Weiss himself was a user of Google Droid and Google Photos (Rivera, on the other hand, neither had a Droid nor a Google Photos account). Weiss First Am. Compl. ¶¶ 26-27; Rivera First Am. Compl. ¶ 26. Between 2013 and 2016, Weiss took "approximately twenty-one" photos of himself while in Illinois on his Droid device. Weiss First Am. Compl. ¶¶ 26-27. These photos were automatically uploaded when they were taken, and then immediately scanned to create a custom face-template based on Weiss's features. *Id.* ¶¶ 28-29. At the time of uploading and scanning, Weiss's Droid was in Illinois and it would have had an Illinois-based Internet Protocol (IP) address. *Id.* ¶ 28.

Both Rivera and Weiss contend that their face-templates were then used by Google to find and group together other photos of them. Rivera First Am. Compl. ¶ 29; Weiss First Am. Compl. ¶ 30. Google also used the templates to recognize their gender, age, race, and location. Rivera First Am. Compl. ¶ 30; Weiss First Am.

Compl. ¶ 31. At no time was Rivera's or Weiss's consent sought by Google to create or use the face-templates. Rivera First Am. Compl. ¶¶ 32-33; Weiss First Am. Compl. ¶ 33-34. Nor did Rivera or Weiss give Google permission to collect or store the data derived from their faces. Rivera First Am. Compl. ¶ 31; Weiss First Am. Compl. ¶ 32.

Based on these allegations, Rivera and Weiss, individually and on behalf of a proposed class, bring suit against Google for a violation of the Illinois Biometric Information Privacy Act. They argue that the face geometry templates created by Google are "biometric identifiers" within the definition of the Privacy Act, and accordingly cannot be collected without consent. Rivera First Am. Compl. ¶¶ 1, 21, 43-48; Weiss First Am. Compl. ¶¶ 1, 21, 44-49. Rivera and Weiss also contend that when the face templates are used to recognize gender, age, and location, Google is collecting "biometric information" within the definition of the Act, which is also forbidden without consent. Rivera First Am. Compl. ¶¶ 1, 23, 43-48; Weiss First Am. Compl. ¶¶ 1, 23, 44-49. Rivera and Weiss finally allege that Google did not make publicly available a biometric data retention and destruction schedule as required by the Act. Rivera First Am. Compl. ¶ 47; Weiss First Am. Compl. ¶ 48. Google now moves to dismiss Plaintiffs' suit for failure to state a claim. *See* Def.'s Mot. to Dismiss; R. 49, Def.'s Br.

II. Standard

Google brings its motion under Federal Rule of Civil Procedure 12(b)(6). A Rule 12(b)(6) motion tests the sufficiency of the complaint, *Hallinan v. Fraternal Order of Police of Chi. Lodge No. 7*, 570 F.3d 811, 820 (7th Cir. 2009); *Gibson v. City of Chi.*, 910 F.2d 1510, 1520 (7th Cir. 1990). When deciding a motion to dismiss, the Court accepts as true all factual allegations in the complaint and draws all reasonable inferences in the plaintiff's favor. *Killingsworth v. HSBC Bank Nev., N.A.*, 507 F.3d 614, 618 (7th Cir. 2007).

Under Rule 8(a)(2), a complaint generally need only include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). The complaint must "give the defendant fair notice of what the ... claim is and the grounds upon which it rests." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (alteration in original) (internal quotation marks and citation omitted). These allegations "must be enough to raise a right to relief above the speculative level," *id.*, and must "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face,'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). Only factual allegations are entitled to the assumption of truth, not mere legal conclusions. *Iqbal*, 556 U.S. at 678-79.

III. Analysis

Google's primary argument is that Rivera and Weiss really are complaining about Google's use of their *photographs*, and the Illinois Biometric Information

Privacy Act does not cover photographs or information derived from photographs. Def.'s Br. at 6-13. Google also offers a backup argument: even if what Google is doing would run afoul of the Privacy Act if done in *Illinois*, Google supposedly did not do anything in Illinois, so there is no violation of that Illinois law. *Id.* at 13-15. And Google offers a backup to the backup argument: if the Privacy Act does purport to cover what Google did outside of Illinois, then the state statute actually conflicts with the federal Constitution's Dormant Commerce Clause. *Id.* at 15-19. Each issue is addressed in turn below.

A. Face Geometry Scans

Google submits that Rivera's and Weiss's claims should be dismissed because the Privacy Act does not apply to photographs or information derived from photographs. Rivera and Weiss, however, argue that face geometry scans created from photographs *are* covered by the Act, and qualify as both "biometric identifiers" and "biometric information" within the Act. So the first question is whether the face geometry scan as described by Rivera and Weiss (a description that must be accepted as accurate at the dismissal-motion stage) fits the statutory definition of either "biometric identifier" or "biometric information." To answer the question, the usual principles of statutory interpretation apply.

Statutory interpretation starts with the plain meaning of the statute's text. *Paris v. Feder*, 688 N.E.2d 137, 139 (Ill. 1997) ("The cardinal rule of statutory construction is to ascertain and give effect to the true intent of the legislature … The best evidence of legislative intent is the language used in the statute itself,

which must be given its plain and ordinary meaning." (citations omitted)). If the text bears a plain meaning, then that is the end of the interpretive exercise, and no other interpretive aids should be used. *People v. Fitzpatrick*, 633 N.E.2d 685, 687 (Ill. 1994). When searching for the statutory text's plain meaning, the overall structure of the statute can provide guidance. *Abrahamson v. Ill. Dep't of Prof'l Regulation*, 606 N.E.2d 1111, 1118 (Ill. 1992). Illinois also follows the interpretive principle that identical words used in different parts of the same statute are generally presumed to have the same meaning. *Baker v. Salomon*, 334 N.E.2d 313, 316 (Ill. 1975). And, when possible, courts should avoid interpreting a statute in a way that renders a word or phrase redundant, meaningless, or superfluous. *People v. Trainor*, 752 N.E.2d 1055, 1063 (Ill. 2001).

Start with the text. The Privacy Act forbids private entities from gathering and keeping a person's "biometric identifier" and "biometric information" without first giving notice and getting consent:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> > (1) informs the subject … in writing that a biometric identifier or biometric information is being collected or stored;
> >
> > (2) informs the subject … in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
> >
> > (3) receives a written release executed by the subject of the biometric identifier or biometric information … .

740 ILCS 14/15(b). Beyond the ban on non-consensual gathering and collecting, private entities that do obtain biometric identifiers and information must publish a "retention schedule" that details how the data will be kept and when it will eventually be destroyed.[5] Victims of a violation may bring a private right of action, with potential recovery set by a statutory damages provision. 740 ILCS 14/20. For a negligent violation, liquidated damages of $1,000 or actual damages (whichever is greater) are available for each instance; for an intentional or reckless violation, the numbers ratchet up to liquidated damages of $5,000 for each violation or actual damages (whichever is greater). *Id.*

But what is a "biometric identifier" and what is "biometric information"? The latter is defined by reference to the former, so it makes sense to start with "biometric identifier." The Act defines "biometric identifier" in a very specific way:

> "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

740 ILCS 14/10. One-by-one, this definition specifies each particular type of covered biometric identifier. This specific, one-by-one listing is different from the many statutory definitions that use general words, like "record, document, or tangible object," 18 U.S.C. § 1519 (interpreted by *Yates v. United States*, 135 S. Ct. 1074, 1086-88 (2015)), or the statutes that list out a set of specific items and then add a broader general word, like "moneys, funds, credits, securities or other things of

[5]"A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a).

value," 18 U.S.C. § 657. In contrast to those definitions, here the Privacy Act defines "biometric identifier" with the *complete* set of *specific* qualifying biometric identifiers. Each specific item on the list, not surprisingly, fits within the meaning of the term "biometric identifier," that is, a biology-based set of measurements ("biometric") that can be used to identify a person ("identifier").

After affirmatively defining "biometric identifier," the Act goes on, in the same long paragraph as the affirmative definition, to list a catalogue of things that are *not* biometric identifiers. The list runs on for five sentences, and the first sentence is especially important for this case because that is where the word "photographs" appears (the bracketed numbers do not appear in the statute, and instead are inserted for convenience):

> **[1]** Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. **[2]** Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. **[3]** Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. **[4]** Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. **[5]** Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

740 ILCS 14/10. Because the parties base some of their arguments on these "do not include" sentences, it is worth noting that some of these sentences do *not* simply set out exceptions, in the usual sense of the word "exceptions," to the specified biometric identifiers. That is, an "exception" to a definition is usually something that otherwise probably *would* be covered by the affirmative definition. To be sure, some of the five disqualifying sentences are true exceptions. For example, in the fourth disqualifying sentence, if a patient will be undergoing facial reconstruction surgery, then the information collected from a face geometry scan—which otherwise would be covered by the affirmative definition of biometric identifier—in that "health care setting" would be exempted from the definition. In contrast, the first sentence says (in part) that "written signatures" are not biometric identifiers. This reads like a "just to be totally sure" disqualifier, rather than an ordinary exception, because it seems unlikely that written signatures could ever fit into any of the affirmatively specified biometric identifiers (to repeat the specified list: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry").

Moving on to "biometric information," the Privacy Act affirmatively defines that term by referring back to "biometric identifier," and then also provides a "does not include" disqualifier:

> "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

740 ILCS 14/10. The affirmative definition of "biometric information" does important work for the Privacy Act; without it, private entities could evade (or at least arguably could evade) the Act's restrictions by converting a person's biometric identifier into some other piece of information, like a mathematical representation[6] or, even simpler, a unique number assigned to a person's biometric identifier. So whatever a private entity does in manipulating a biometric identifier into a piece of information, the resulting information is still covered by the Privacy Act if that information can be used to identify the person.

Turning to the case at hand, as alleged in the First Amended Complaints (the truth of which must be assumed for now), the "face templates" (as Rivera and Weiss call them) generated by Google do qualify as a "biometric identifier" under the Privacy Act. For each face template, Google is creating a set of biology-based measurements ("biometric") that is used to identify a person ("identifier"). More importantly, as alleged, a face template is one of the specified biometric identifiers in the Privacy Act, namely, a "scan of … face geometry." 740 ILCS 14/10.

Against this straightforward reading of the definition of "biometric identifier," Google argues that face-scan measurements derived from a photograph do not qualify as biometric identifiers. Def.'s Br. at 1. In Google's view, only face scans that are done *in person* can qualify as biometric identifiers. *Id.* at 7; R. 52, Def's. Reply Br. at 5. But nothing in the text of the Privacy Act directly supports

[6]Iris-recognition systems, for instance, might use "iris codes" derived from iris images in scans. *See, e.g.*, Kim Zetter, *Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners*, Wired (July 25, 2012), http://www.wired.com/2012/07/reverse-engineering-iris-scans.

this interpretation. Nothing in the statute says, one way or the other, *how* the biometric measurements must be obtained (or stored, for that matter) in order to meet the definition of "biometric identifier." The definition simply lists the specific identifiers that are covered. And the particular biometric identifiers can, in fact, be collected in various ways without altering the fact that the measurements still are biometric identifiers. Consider, for example, fingerprints: the definition is indifferent as between inked fingerprints versus digital images of fingerprints. Nor does the definition say whether a scan of face geometry has to be in person or may be generated from a photograph or a video.[7] Indeed, because advances in technology are what drove the Illinois legislature to enact the Privacy Act in the first place, it is unlikely that the statute sought to limit the definition of biometric identifier by limiting *how* the measurements are taken. Who knows how iris scans, retina scans, fingerprints, voiceprints, and scans of faces and hands will be taken in the future? It is not the how that is important to the Privacy Act; what's important is the potential intrusion on privacy posed by the unrestricted gathering of biometric information. The bottom line is that a "biometric identifier" is not the underlying

[7]Google does correctly argue that previous district-court cases analyzing the Privacy Act are not binding on this Court (just as this Opinion is not binding on other courts), Def.'s Br at 11-12, and the Court does not treat them as binding. *See Norberg v. Shutterfly, Inc.*, 2015 WL 9914203 (N.D. Ill. Dec. 29, 2015) (denying motion to dismiss face template claim); *In re Facebook Biometric Info. Privacy Litig.*, 2016 WL 2593853 (N.D. Cal. May 5, 2016) (drawing a distinction, which this Opinion does not adopt, between digital photographs and physical photographs). Three other face template cases brought under the Illinois Biometric Information Privacy Act have been dismissed, but on other grounds. *Gullen v. Facebook.com, Inc.*, 2016 WL 245910 (N.D. Ill. Jan. 21, 2016) (lack of personal jurisdiction); *Vigil v. Take–Two Interactive Software, Inc.*, 2017 WL 398404 (S.D.N.Y. Jan. 30, 2017) (lack of standing); *McCollough v. Smarte Carte, Inc.*, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016) (lack of standing).

medium itself, or a way of taking measurements, but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person.

Without direct textual support in the affirmative definition of "biometric identifier," Google's argument hinges on the first "do not include" sentence in the definitional paragraph of "biometric identifier." Remember that the affirmative definition is followed by five sentences that say what biometric identifiers "do not include." The first of those sentences includes "photographs" in the list of what biometric identifiers do not include:

> Biometric identifiers do not include writing samples, written signatures, *photographs*, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.

740 ILCS 14/10 (emphasis added). With that premise in hand—photographs are not biometric identifiers—Google then points to the "do not include" sentence from the definition of biometric *information*. Remember that sentence says, "Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers." *Id.* So, Google's argument continues, biometric information does not include information derived from photographs, because photographs are excluded from the definition of biometric identifiers. But Google's argument is not yet complete, because Rivera and Weiss are *not* alleging that the photographs themselves are the biometric identifiers, and because Google still needs to grapple with the face templates—not the photographs—qualifying as biometric *identifiers*. To do this, Google purports to find a "careful structure," Def.'s

Br. at 8, in the separate definitions of "biometric identifier" and "biometric information." Google argues that the two definitions distinguish the "source of the content":

> what is derived from a person is a "biometric identifier," and what is subsequently derived from a biometric identifier is "biometric information." The statute's structure thus confirms that a "scan of … face geometry" must be derived from the person herself. Plaintiffs' reading of the statute would collapse this careful structure, rendering the distinction between "biometric identifier" and "biometric information" meaningless.

Id. In essence, Google is arguing that if biometric *information* cannot be "based on" something from the biometric-identifier paragraph's "do not include" list (for example, "photographs"), then an *identifier* may also not be "based on" something from that same list.

The problem with this argument is that there is no textual or structural clue to support it. The definition of "biometric identifier" does *not* use words like "derived from a person," "derived in person," or "based on an in-person scan," whereas the definition of "biometric information" does say that it is information "based on" a biometric identifier. So there is no parallel structure to speak of. It would have been simple enough for the Illinois legislature to include similar "based on" or "derived from" language in the definition of "biometric identifier," but it did not. As discussed earlier, the things on the list of biometric identifiers are just that—specific, biology-based measurements used to identify a person, without reference to how the measurements were taken. And, as noted above, the "biometric information" goes on to ensure that private entities cannot do an end-around the Privacy Act by converting biometric identifiers into some other format. So, contrary to Google's

position, there *is* a meaningful distinction between identifiers and information (one being the set of biometric measurements, the other being a conversion of those measurements into a different, useable form), and that distinction has nothing to do with the "careful structure" that Google describes.

The other fatal problem with Google's "careful structure" argument is that it depends on drawing some structural meaning from the "do not include" sentences. But that cannot be done. As noted earlier, the five sentences in the run-on paragraph (block quoted earlier in the Opinion) comprise a mix of things that are true exceptions (that is, they otherwise would qualify as a biometric identifier) and others that read more like just-to-be-sure exclusions. Yes, structure and context can provide interpretive help, but the "do not include" listings defy a common thread that sheds any additional light on the straightforward affirmative definition of biometric identifier. As a result, it is not sensible to use the photograph exclusion to back-fill an interpretation of biometric identifier—unless, of course, the proposed identifier in question is simply a photograph. But a photograph is just that—a photograph, *not* a scan of face geometry, which is a set of biology-based measurements. Rivera and Weiss nowhere argue that the photograph itself is the biometric identifier. Indeed, if Google simply captured and stored the *photographs* and did not measure and generate scans of face geometry, then there would be no violation of the Act. (The same is true of someone, say a journalist, who records a person's voice without generating a voiceprint.) All in all, the reference to "photographs" in the first "do not include" sentence is no help to Google's argument.

Google's final attempt to argue from text and structure is premised on the Privacy Act's written-consent requirement. 740 ILCS 14/15(b)(3). That requirement dictates that, in order to collect a person's biometric identifier or biometric information, a private entity must (among other things) receive a "written release" executed by the person. *Id.* The need for a written release is telling, Google says, because consent may be most easily and clearly given in person. Def.'s Br. at 9.

This is unconvincing for two reasons. First and foremost, even assuming, for the moment, that in-person consent is logistically more convenient to get than remote consent, the absence of any other textual or structural clues that the scan must be in person outweighs the weak inference arising from any purported logistical convenience. Second, there is substantial reason to doubt just how much easier it is to obtain a written release in person. Many courts, for instance, have routinely upheld one-click ("clickwrap") consent features on websites and internet services. *See, e.g.*, *Van Tassell v. United Mktg. Grp., LLC*, 795 F. Supp. 2d 770, 790 (N.D. Ill. 2011) (courts "regularly uphold" clickwrap agreements when structured properly); Ronald J. Mann & Travis Siebeneicher, *Just One Click: The Reality of Internet Retail Contracting*, 108 COLUM. L. REV. 984 (2008) (profiling "one-click" web agreements). Agreeing to a written release remotely will, in many instances, be easier to obtain than in person. And the written-release requirement applies *not* just to the private entity that directly collects or captures the biometric identifier; the requirement also applies to any private entity that "purchase[s], receive[s] through trade, or otherwise obtain[s]" a biometric identifier or biometric

information. 740 ILCS 14/15(b). So those private entities would have to obtain a written release as well, and there is no reason to think that obtaining a release from someone—perhaps long after the initial collection of the biometric identifier or biometric information—is easier to do in person rather than remotely.

Because the text of the Privacy Act provides the answer to whether the alleged face templates come within the definition of biometric identifier, there is no need to resort to legislative history. *Ultsch v. Ill. Mun. Ret. Fund*, 874 N.E.2d 1, 10 (Ill. 2007) ("Where the language of a statute is plain and unambiguous, a court need not consider other interpretive aids."). For the sake of completeness, however, the Court explains why Google's legislative-history-based arguments are also wanting.

Google first points to the statement of the Act's cosponsor on the floor of the state House of Representatives to argue for the importance of the in-person aspect of scans. Def.'s Br. at 10. The state Representative declared that the bill's urgency was exemplified by the bankruptcy of a company called Pay By Touch, which was "the largest fingerprint scan system in Illinois." *Id.* (quoting IL H.R. Tran. 2008 Reg. Sess. No. 276 at 249 (May 30, 2008)). The bankruptcy, according to the Act's cosponsor, left "thousands of customers … wondering what will become of their biometric … data." *Id.* Even if legislative history could be relied on here, this is but one House floor statement. Indeed, here there is no mystery on the subject of legislative intent, because the Act *itself* clearly sets forth legislative findings and legislative intent. Section 5 is entitled, "Legislative findings; intent," and elaborates on the legislature's concerns. To be sure, the only *example* given in Section 5 relates

to in-person transactions ("finger-scan technologies at grocery stores, gas stations, and school cafeterias"), 740 ILCS 14/5(b), but the stated concern is considerably broader than this one application. That same Section declares that the General Assembly finds that the "use of biometrics is growing in the business and security screening sectors" and that major corporations are testing "new applications of biometric-facilitated financial transactions." *Id.* § 14/5(a)-(b). Section 5 also outlines the unique threats of biometrical information capture (for example, the uniqueness and unalterable nature of such information, the risks for identity theft, and the chance that concerned citizens will avoid biometric-facilitated transactions). *Id.* § 14/5(c), (e). And the Section goes on to point out that "[t]he full ramifications of biometric technology are not fully known." *Id.* § 14/5(f). All of this explicit statutory text dwarfs Google's single floor statement.

Google next argues that the legislative history would have recorded some reaction to this proposed Act—"someone would have remarked upon it"—if the legislation were truly so allegedly "sweeping" as Rivera and Weiss suggest (that is, that it covers face templates scanned from photographs). Def.'s Br. at 10. This line of thinking is not persuasive. Google calls the reading "sweeping" because it argues that the Act would, under the Plaintiffs' reading, apply to "any individual … running common photo-organizing software on a home computer." *Id.* For two reasons, however, this is an unconvincing legislative-history argument. First, it is not clear that face-scanning technology on home computers was actually so ubiquitous in 2008 (when the bill was under consideration) that legislators would

have considered the Act's impact on home-computer users. Second, it is not clear that the Act would even apply to an ordinary user who is simply organizing photos on a home computer, unless that person is running a self-created program to measure faces in photographs. More likely, someone on a home computer, if using any face-scan technology at all, would be doing so through an already established program or service similar to Google Photos. Perhaps Illinois courts will interpret the Act's primary restriction—no private entity may "collect, capture, purchase, receive through trade, or otherwise obtain" a biometric identifier or biometric information without a written release—to not apply to the run-of-the-mill home-computer user who is not directly doing the collecting, capturing, purchasing, trading for, or obtaining of the protected identifier or information. Or perhaps Illinois courts will interpret the statute's damages provisions as not applying to the ordinary home-computer user because there is no negligence, recklessness, or intent to violate the Act. 740 ILCS 14/20(1)-(2) (authorizing recovery of damages only where there is negligence, recklessness, or intent). The point is that the absence of the home-computer scenario from the annals of legislative history is not telling.[8]

[8]In a nod to Sherlock Holmes, Google calls the absence of references to home-computer users "the dog that did not bark." Def.'s Br. at 10 (quoting *Chisom v. Roemer*, 501 U.S. 380, 396 n.23 (1991)). In *Silver Blaze*, Sir Arthur Conan Doyle no doubt made an excellent point by colorfully describing how an *omission* can be telling. But there is reason to doubt the validity of that common-sense observation when it comes to legislative history. Google cites to a footnote in *Chisom* which, in turn, cites a dissent in *Harrison v. PPG Industries, Inc.*, 446 U.S. 578, 602 (1980) (Rehnquist, C.J., dissenting). But the majority opinion in *Harrison* casts doubt on the usefulness of the silence-is-telling principle when reading legislative history: "it would be a strange canon of statutory construction that would require Congress to state in committee reports or elsewhere in its deliberations that which is obvious on the face of a statute. In ascertaining the meaning of a statute, a court

And even if applying the Act to ordinary individuals might be a good reason to amend the Act, it is not a reason to depart from the plain meaning of the statutory text.

Google next argues that the General Assembly's ultimate rejection of other proposed words in the statute's definitions also speaks to the legislature's intent to exclude facial geometry data-gathering not done in person. More specifically, Google points out that the Assembly's "opt[ing] for the word 'scan' over 'records' suggests that it cared about how the content was obtained." Def.'s Br. at 10-11. Google contends that a scan "suggests something done to the person herself" and "records" does not. *Id.* at 11; Def.'s Reply Br. at 7. This is not necessarily right. "Scan" may indeed be more suggestive of a direct procedure than the more inert-sounding "record." But within the various meanings of "scan" in everyday speech, "scan" is not obviously more suggestive of something done directly to a *person* than to a *thing* (like a photograph). And, most importantly (as discussed earlier), the definition of biometric identifier is simply a list of specified things that does not distinguish the manner in which the identifier is generated.

Google's final point on legislative history is that the General Assembly dropped, at some point, the word "facial recognition" from an earlier-proposed definition of "biometric identifier." Def.'s Br. at 11. But Google offers no legislative explanation of *why* the term was dropped. For all the legislative history shows, the term was dropped simply because it was redundant with "facial geometry." Or (and

---

cannot, in the manner of Sherlock Holmes, pursue the theory of the dog that did not bark." *Id.* at 592.

this shows the weakness of relying on unexplained legislative history) perhaps the term was dropped because it did not make grammatical sense. The proposed phrase really read like this: "records or scans of … facial recognition." R. 49-1, Exh. D at 2-3. A "scan of facial recognition" is arguably not even grammatically correct wording. In any event, the removal of "facial recognition" does not tell us anything about whether Google's face templates are implicated by the statute or not. "[S]cans" of "face geometry" made it into the final version, and those, as described above under a plain-meaning interpretation of the statute, can apply equally to in-person and photograph-based biometric measurement of faces.[9]

All of this said, it remains possible that Google could prevail on its face-template arguments (that is, that what Google collects from the photos are not covered by the Act) once further factual development has occurred in discovery. It is conceivable that discovery will reveal that what Google is *actually* doing does not fit within the definition of biometric identifier as interpreted by the Court. Until that time, however, the Plaintiffs' allegations must be taken as true, and they adequately state a claim under the Privacy Act.

B. Presumption Against Extraterritoriality

Google's second argument in its motion to dismiss is that the Plaintiffs' claims cannot proceed because applying the Privacy Act to Google would result in an extraterritorial application of the statute. Def.'s Br. at 13. In other words, this

[9]Google also refers to legislative "history" in the form of what happened *after* the Privacy Act's enactment. Def.'s Br. at 3 n.3 (summarizing HB 6074, S. Floor Amend. No. 1, 99th Gen. Assemb., Reg. Sess. (Ill. May 26, 2016)). But Google does not cite to controlling Illinois case law establishing that post-enactment proposals (rejected ones, at that) are valid statutory interpretation tools.

Illinois law applies only in Illinois, and Google is not doing anything in Illinois. As explained in this section, at this early stage in the case, the Court cannot decide this issue in Google's *factual* favor, and can only hold—as a matter of *law*—that the Illinois Biometric Information Privacy Act does not apply extraterritorially. Discovery is needed to determine whether there are legitimate extraterritoriality concerns.

Under Illinois law, an Illinois statute does not have extraterritorial effect unless the Assembly expressly intended it. *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 852–53 (Ill. 2005) (quoting *Dur–Ite Co. v. Indus. Comm'n*, 68 N.E.2d 717, 722 (Ill. 1946)). Google is correct that, with regard to the Privacy Act, there is no sign of that sort of intent from the Illinois legislature. Nor does Rivera or Weiss argue that the Act is intended to operate extraterritorially. The Privacy Act is not authorized to have extraterritorial effect.

If the Act cannot apply extraterritorially, then Rivera's and Weiss's asserted violations of the Act must have taken place in Illinois in order for them to win. Returning to *Avery* (on which both parties rely for their arguments on the location of the ostensible Privacy Act violations),[10] there the Illinois Supreme Court explained that "there is no single formula or bright-line test for determining whether a transaction occurs within this state." 835 N.E.2d at 854. Instead, a court

[10]Although *Avery* specifically dealt with Illinois's Consumer Fraud and Deceptive Business Practices Act, its reasoning on whether a transaction occurred in Illinois in determining extraterritoriality concerns has since been used for other Illinois statutory claims. *See, e.g.*, *Specht v. Google, Inc.*, 660 F. Supp. 2d 858, 866 (N.D. Ill. 2009) (*Avery* used for assessing an Illinois Deceptive Trade Practice Act claim). As the Illinois Biometric Information Privacy Act has no developed case-law on this point, the Court will borrow the *Avery* totality-of-the-circumstances standard here as well.

must analyze whether "the circumstances relating to the transaction occur primarily and substantially" within Illinois. *Id.* at 853. Circumstances will vary in every case but the factors considered in *Avery* (assessing an Illinois Consumer Fraud Act claim) are instructive: the residency of the plaintiff, the location of harm, communications between parties (where sent and where received), and where a company policy is carried out. *Id.* at 854; *see also Gros v. Midland Credit Mgmt.*, 525 F.Supp.2d 1019 (N.D. Ill. 2007) ("It is … incorrect [in determining whether a disputed transaction occurred in Illinois] to focus on only one aspect of the disputed transaction.").

Much of this case revolves around conduct occurring online or on a "cloud." *Avery*'s totality-of-the-circumstances standard has not yet produced much guidance in the context of online conduct. In one case applying *Avery* to an Illinois Deceptive Trade Practice Act claim, the court found that an infringement that "took place on the Internet and was international in scope" was thereby "presumably occurring in Illinois." *Specht v. Google, Inc.*, 660 F. Supp. 2d 858, 866 (N.D. Ill. 2009). That assessment, in combination with other Illinois connections, was found sufficient to state a claim under that particular statute. *Id.* In another case, a London-based plaintiff was surfing a hotel's website to book a hotel room in Moscow. Later taking issue with allegedly misleading prices quoted on that website, that plaintiff sued the hotel on an Illinois Consumer Fraud Act claim in Illinois, arguing that *Avery* had been satisfied because the hotel company's principal place of business was in Illinois and because the hotel website had an Illinois choice of law clause. *Shaw v.*

Hyatt Int'l Corp., 2005 WL 3088438, at *2–3 (N.D. Ill. Nov. 15, 2005), *aff'd*, 461 F.3d 899 (7th Cir. 2006). The district court found those connections too tenuous and decided the relevant transaction should not be found to have "primarily and substantially" occurred within Illinois. *Id.* Neither of these cases is directly controlling, but they show that Internet factors (site access, corporate operation of a website) might be part of the *Avery* calculus.

The question, then, is whether Google's activities—making face templates of Rivera and Weiss in photographs uploaded automatically from Google Droid devices in Illinois—are an extraterritorial (and therefore not-actionable) application of the Privacy Act. According to Rivera and Weiss, all of the following are Illinois connections: Rivera and Weiss are Illinois residents, R. 51, Pls.' Resp. Br. at 22; Rivera's and Weiss's photographs were taken in Illinois, *id.*; and Rivera's and Weiss's photographs were allegedly "automatically uploaded in Illinois to the cloud-based Google Photos service … from an Illinois-based Internet Protocol ('IP') address," *id*. Rivera and Weiss also allege that it was in Illinois where Google failed to provide Rivera and Weiss with required disclosures and failed to get Rivera's and Weiss's consent, *id.* at 22-23. At this stage of the proceedings we take the Plaintiffs' allegations as true, and these alleged facts tip toward a holding that the alleged violations primarily happened in Illinois.

Google contends that the face scans did not occur "primarily and substantially" in Illinois. Def.'s Br. at 14. It cites to Rivera's and Weiss's failure to allege a location for the actual scanning of face geometry. *Id*. In Google's reckoning,

the location of the scan ("the place where a biometric identifier is 'collected, captur[ed], … or otherwise obtained'") is to be seen as the determinative "situs" of the Privacy Act violation. *Id.*; Def.'s Reply Br. at 11. Google also cites other circumstances not mentioned by Rivera or Weiss that could be relevant under the *Avery* test, such as "where the photographer resides" (in the case of Rivera) and "where the Google Photos user signed up for Google Photos" (in the case of Weiss). Def.'s Br. at 14.

Assessing these arguments at this initial stage, the Court concludes that the Plaintiffs sufficiently allege facts that would deem the asserted violations as having happened in Illinois. But there is no bright-line rule for determining this, so the parties will have the chance to develop more facts during discovery. For example, where did the alleged scans actually take place? Even if we do definitely determine that the scanning takes place outside of Illinois, that would not necessarily be dispositive. *Avery*, 835 N.E.2d at 853 ("The place of injury or deception is only one of the circumstances that make up a fraudulent transaction and focusing solely on that fact can create questionable results. If, for example, the bulk of the circumstances that make up a fraudulent transaction occur within Illinois, and the only thing that occurs out-of-state is the injury or deception, it seems to make little sense to say that the fraudulent transaction has occurred outside Illinois."); *Gros*, 525 F.Supp.2d at 1024 ("*Avery* instructs courts to consider the totality of the circumstances in determining whether the disputed transaction occurred 'primarily

and substantially' in Illinois. … It is therefore incorrect to focus on only one aspect of the disputed transaction.").

Another issue needing further factual refinement is where precisely the lack of consent took place. This is a complex issue, and neither side has yet addressed it thoroughly. Part of the lack of consent location issue may hinge on whether uploads are indeed scanned "immediately" as Rivera and Weiss suggest or if there is any intervening time before a scan occurs.[11] In that intervening time (even if short), the subject of a photo could leave the state of Illinois (which in that case would mean that the scan and the associated failure to get consent happened when the person was in a different state). These factors would also not be dispositive, but they would be worth considering for the *Avery* test. For now, it is enough to say that the allegations survive the accusation that the law is being applied outside of Illinois.

C. Dormant Commerce Clause

Google's last argument is that the practical effect of the Illinois Biometric Information Privacy Act, if read the way Rivera and Weiss read it, would violate the Dormant Commerce Clause of the United States Constitution. Def.'s Br. at 15. Google reaches that conclusion by arguing under an extraterritorial Dormant Commerce Clause theory that the Privacy Act (if read the way Plaintiffs read it) has the practical effect of controlling conduct beyond Illinois's boundaries. *Id.*

The Constitution grants Congress the power to "regulate Commerce with foreign Nations, and among the several States, and with the Indian tribes." U.S.

[11]Neither side is arguing that for the purposes of the Privacy Act, Google needed consent to upload the photographs to the cloud. It is only the collection of the biometric identifier (the scan) that requires consent.

Const. art. I, § 8, cl. 3. The United States Supreme Court has long interpreted in this clause a corresponding negative command (the "Dormant Commerce Clause") prohibiting some state laws that burden interstate commerce even when Congress has not legislated on a subject. *Okla. Tax Comm'n v. Jefferson Lines, Inc.*, 514 U.S. 175, 179 (1995). A state statute violates the commerce clause "[w]hen a state statute directly regulates or discriminates against interstate commerce, or when its effect is to favor in-state economic interests over out-of-state interests." *Brown-Forman Distillers Corp. v. N.Y. State Liquor Auth.*, 476 U.S. 573, 579 (1986). A statute may also violate the clause even if it is not directly protectionist: "[w]hen, however, a statute has only indirect effects on interstate commerce and regulates evenhandedly, we have examined whether the State's interest is legitimate and whether the burden on interstate commerce clearly exceeds the local benefits." *Id.*

A third test—based on extraterritorial effects—has been used increasingly by courts to assess compliance with the Commerce Clause. In *Healy v. Beer Institute, Inc.*, the Supreme Court laid out the Commerce Clause's implications for extraterritoriality in state regulation:

> [1] [the] Commerce Clause ... precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State;
>
> [2] a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State; and

> [3] the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation.

491 U.S. 324, 336 (1989) (bracketed numbers and paragraphing added). *See also Midwest Title Loans, Inc. v. Mills,* 593 F.3d 660, 665 (7th Cir. 2010) ("But another class of nondiscriminatory local regulations is invalidated without a balancing of local benefit against out-of-state burden, and that is where states actually attempt to regulate activities in other states."); *Int'l Dairy Foods Assoc. v. Boggs,* 622 F.3d 628, 646 (6th Cir. 2010) ("a state regulation is 'virtually *per se* invalid' if it is ... extraterritorial ... in effect."); *Pac. Merch. Shipping Ass'n v. Goldstene,* 639 F.3d 1154, 1178 (9th Cir. 2011) ("[T]he Commerce Clause prohibits state legislation regulating commerce that takes place wholly outside of the state's borders, regardless of whether the commerce has effects within the state.").

Google argues that under this extraterritoriality test, the Privacy Act as construed by Rivera and Weiss violates the Commerce Clause. Google gives an elaborate hypothetical to show that a very tenuous connection to Illinois (merely driving through the state and uploading a photograph that had nothing to do with Illinois) could still lead to a violation of the Act. Def.'s Br. at 15. It also argues that, if there is not a bright-line rule for determining for the purposes of the Act whether conduct is taking place in Illinois, Google will be forced to comply with the Act nationwide to avoid possible liability. *Id.* at 16. Google then argues that laws attempting to regulate the Internet pose unique constitutional dangers, *id.* at 17,

and that Illinois's Privacy Act would trench on the rights of other states to make their own regulation (or lack thereof) on biometric data, *id.* at 17-18.

Again, however, this is not the stage at which to assess these arguments in detail. The Commerce Clause argument is directly related to the extraterritoriality effect argument treated above. To repeat, the Illinois Biometric Information Privacy Act was not intended to and does not have extraterritorial application. Whether the Privacy Act is nevertheless being summoned here to control commercial conduct wholly outside Illinois is not possible to figure out without a better factual understanding of what is happening in the Google Photos face-scan process. What is learned from discovery there will inform both the more general extraterritoriality analysis above and this Dormant Commerce Clause analysis.

In addition to the factors needing discovery mentioned earlier, one of the arguments unique to the Commerce Clause section also warrants further factual development. Specifically, the parties need to develop what Google's burdens of compliance would actually be under the Privacy Act, if it were read in the way the Plaintiffs suggest. As noted earlier, the Privacy Act only subjects violators to statutory damages if there is negligence or willfulness. 740 ILCS 14/20. So even if the Plaintiffs' construction of the Act were to depend on a totality-of-the-circumstances test for assessing location, Google could conceivably avoid liability by taking reasonable steps toward compliance. But perhaps the technological details of Google Photos' operation and the ubiquity of the Internet and cloud computing would make even attempts at reasonable compliance unworkable. Again, further

discovery could help determine if that is so. It would also allow the Court to see in more detail how Google's specific transactions fit into the current legal landscape on Internet-based Commerce Clause violations.

IV. Conclusion

Google's motion to dismiss is denied. At the next status hearing, the Court will set the discovery schedule.

ENTERED:

s/Edmond E. Chang
Honorable Edmond E. Chang
United States District Judge

DATE: February 27, 2017